DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY SUPPORT ACTIVITY AREA III
UNIT # 15716
APO AP 96271-0716

REPLY TO
ATTENTION OF:

EANC-HG-CDR (380a) 11 June 2002

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: USASA Area III Policy Memorandum #26, Information Assurance Policy

1. This policy **supersedes** the USASA Area III Policy Memo #26, SAB, dated **23 Oct 01**.

2. **References**:

a. Army Regulation 380-19, Information Systems Security, 27 Feb 98.

b. Army Regulation 25-1, Army Information Management, 15 Feb 00.

c. DA Message, Subject: Network Security Improvement Program (NSIP) Anti-viral Update Policy, P201150Z JUL 99.

d. EUSA Pamphlet 25-50, Information Management Officer's Handbook, 24 Oct 00.

e. EUSA Regulation 25-3, Information Assurance Program, 30 Aug 99.

f. 19th TSC Memorandum, Subject: Email Classification Banner, 12 Mar 00.

3. **Purpose**: To establish policy for access to any Automated Information Systems (AIS) and network in USASA Area III. AIS are defined as any computer to include laptops, Personal Electronic Devices (PEDs), and Personal Digital Assistants (PDAs).

4. **Applicability**: This policy memorandum applies to all KN employees, US military, and US civilian personnel assigned or attached to USASA Area III and any visitors utilizing any AIS or Local Area Network (LAN) managed in this command.

5. **Policy**:

a. All AIS users assigned or attached to USASA Area III will participate in domain authentication. All systems will be configured to mandate login to the USASA Area III domain. Newly assigned personnel will report to their Information Management Office as part of their inprocessing for an Information Systems Security Brief (ISSB) and to obtain a domain login identification and password and to apply for an email account. All users are required to be familiar and comply with DOD, EUSA, and 19th TSC IA/IMO policy available on the Intranet at https://usasaa3im017 or https://160.135.51.17.

b. Any guests not assigned to USASA Area III requiring access to any network must read the ISSB and report to the Information Management Office to sign the log. Passwords for email or network access will not be shared and is prohibited by AR 380-19. An Information Assurance Security Officer (AISO) or Information Management Office personnel must scan all removable media (floppy disks, Zip disks, etc.) that guests may bring for viruses before they are used in any AIS in this command.

c. Any visiting AIS user that brings any AIS (desktop or laptop) and plans to connect to any LAN must have it audited for the most recent Antivirus software and definitions by the ISSO or IMO personnel before connecting it to a LAN or receiving an IP address.

d. Privately owned personal computers will not be connected to any government LAN.

e. All current and newly purchased Area III desktop and notebook computers will conform to the EUSA Computer Security Configuration Baseline (CSCB) and Area III Symantec AntiVirus Enterprise System before being operated and connected to any LAN. The Information Management Office must ensure that the computer conforms to this standard before the system and network are accessed. Under no circumstances will a new system be connected to the LAN or operated without approval from the IAM. Contractor or PM fielded systems must have an SSAA (generic accreditation) or IATO (Interim Authority To Operate) before being connected to any LAN.

f. All systems and laptops will be in compliance with the following Area III Operating System and Application standards:

Windows NT/2000
Internet Explorer 6.0
Acrobat 5.0
FormFlow Filler 2.23

Norton Antivirus Corporate Edition 7.51
MS Office 2000 or XP Professional
EasyZip 2000 ver 4.0 (freeware)
Microsoft Exchange/Outlook 2000/XP

g. Systems running operating systems other than Windows NT/2000 will not be connected to the network. Users with systems running applications not listed above must comply with AR 380-19 and seek approval from the IAM and IMO to operate the software on an Area III system. All software used on any government system must be government owned. Exceptions to the Windows NT operating system due to operational requirements will be made on a case-by-case basis with the associated risk included in the accreditation submitted to the Designated Approving Authority.

h. All systems and laptops are required to have the Logon Screen Saver selected with password protection enabled and set to lock after a period of inactivity not to exceed 15 minutes. Windows NT users will lock their workstations whenever away from their system using the Control-Alt-Delete keys and selecting Lock Workstation.

i. Users will not enable BIOS passwords to prevent access to their government-owned computer by IMO/IA personnel. Furthermore, keyboard and mice will not be physically secured to prevent authorized access to any government-owned computer.

j. All systems and laptops will have the unclassified email banner software installed. This software causes Exchange or Outlook to prompt the user to insert an UNCLASSIFIED label in the header and body of the message before it is sent. This provides a visual reminder for us to pay attention to what we are sending over the unclassified system.

k. File and directory sharing to include web or FTP services is not permitted on any user system in this command. All sharing will be performed only at the server level where security is centralized. The domain controller or server that the user logs into will provide shared staff folders. Users can copy files and share information through the network using their staff folder. Users will ensure that data placed on the server in these shared staff folders is restored daily to the system assigned to the user who created or maintains the data. The domain controller or server is not currently configured to handle mass storage or massive data backup.

l. All directorates and commands must assign an Information Assurance Security Officer (IASO) and have one appointed on orders for each building at all times. Appointed IASOs will provide their orders to the Information Assurance Manager (IAM), attain certification within 30 days of appointment, attend all training when directed, and support the IAM when requested.

6. **Responsibility**:

a. Staff Directors and Supervisors. Exercise supervision, ensuring all personnel understand and adhere to this and DOD, EUSA, and 19th TSC policies and SOPs.

b. Information Assurance Manager. Enforce this and DOD, EUSA, and 19th TSC IA/IMO policies and SOPs in this command and report any suspicious activity or virus incidents to the local DOIM and Regional Computer Emergency Response Team – Korea.

c. Information Assurance Security Officers (IASOs). Execute your duties listed in AR 380-19, support the Information Assurance Manager (IAM) in his duties, and report any suspicious activity or security violations to the IAM immediately.

d. All USASA Area III Personnel. Comply with this policy and ensure these security guidelines are followed. Report any suspicious activity or security violations to your IASO or directly to the IAM.

7. **POC** is Mr. Javier Lopez, Info Assurance Mgr, IMO, USASA Area III at DSN **753-8920**.

Michael D Clay 11 Jun 02
MICHAEL D. CLAY
COL, IN
Commanding

DISTRIBUTION:
A